The Bill Blackwood
Law Enforcement Management Institute of Texas

==========

Computer Forensics Labs: Enhancing Law Enforcement's Capabilities to Investigate Computer Related Crimes

==========

An Administrative Research Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

==========

By
Charles E. Richmond II

Mesquite Police Department
Mesquite, Texas
June 10, 2004

ABSTRACT

A computer forensics lab provides advanced technology for crime scene processing through the use of digital photography and the ability to analyze computer data in cases that involve pedophiles, homicides, financial crimes, forgeries, and theft on the Internet. Law enforcement has fallen behind in the computer age and regrettably fails to comprehend computer crime and the local impact that it has on communities. An area that is increasingly becoming a financial burden to our citizens and the business community are the area of identity theft and personal account thefts. It is concluded that a computer forensics lab is a necessary investigative tool to meet the demands of the 21st century and investigating crimes committed in Cyberspace.

TABLE OF CONTENTS

Page

INTRODUCTION

Law enforcement agencies at all levels are consistently seeking new technology and innovative ways to enhance their capabilities to provide better service to their communities. Computers have become a part of every day life, being utilized to maintain data for legal and illegal operations. The introduction of computers and the Internet (Cyberspace) into our society and our dependence upon information technology and information infrastructure has created a threat to our national security and economy (The National Strategy to Secure Cyberspace, 2003). The nation's critical infrastructures are vulnerable to attack and disruption through Cyberspace. The nervous system of the nation's critical infrastructures and the control system of our country is Cyberspace (The National Strategy to Secure Cyberspace, 2003). According to the National Strategy to Secure Cyberspace (2003), some of the critical components of the nation's infrastructure are composed of public and private institutions in the areas of; banking and finance, postal and shipping, agriculture, food, water, government, chemicals and hazardous materials, public health, emergency services, and the defense industrial base. Due to these critical components, the National Strategy to Secure Cyberspace (2003) further explained that it is imperative that the local law enforcement agencies and the private sector become involved in protecting these critical areas. The local law enforcement agencies must attempt to control the criminal element through prosecution and the private sector must install systems hardware and internal security measures to protect their corporation's information and assets. President George W. Bush signed the Homeland

Security Act of 2002, which established the Department of Homeland Security (DHS), on November 25, 2002. The DHS will be responsible for several of the initiatives that were created by the National Strategy to Secure Cyberspace.

Due to the vast increase in computer technology, potential threats to our national security, and the illegal activities conducted on the Internet, the establishment of computer forensics labs has evolved. Although computer forensics labs are not a recent development, the establishment at the local law enforcement level has been slow. A computer forensics lab provides advanced technology for crime scene processing through the use of digital photography and the ability to analyze computer data in cases that involve pedophiles, homicides, financial crimes, forgeries, and theft on the Internet. These types of labs will provide investigative information that was not previously available, and will provide a better management of resources and better service to the community.

This project will attempt to answer the question: Is there a need to establish computer forensics labs at the local law enforcement level to enhance its investigative capabilities in providing service to their communities? There has been a standard approach to investigative techniques (not considering or processing potential evidence stored on computers), which does not allow for the introduction of new technology such as computer forensics labs and does not meet the needs for crimes committed on the Internet. These types of labs would greatly accent the present investigative technical capabilities such as Automated Fingerprint Identification System (AFIS). When crime scene investigators process a crime scene, the investigators generally use a 35mm camera to take

photographs, draw diagrams, and attempt to process latent prints, to name a few. These procedures may still have purpose, however the use of digital photography would provide superior viewing quality. Additionally, digital photography would provide the capabilities of viewing the evidence at different angles without tainting the evidence, which may provide evidence that would not have been discovered. Other uses of computer forensics labs would be in the areas of crimes committed through the Internet. There is a tremendous amount of incidents that involve pedophiles contacting children on the Internet, which have led to the sexual assault of children and child pornography websites being established. Computer forensics labs would provide the capabilities to examine suspect computers for information, even if it has been deleted, to assist investigators in building their case for prosecution. The examination of suspect computer information such as e-mails could even enhance investigations of homicides and child abductions.

This project will use information derived from Internet search, books dedicated to this area, police periodicals, surveys, and interviews to gather information about the benefits of establishing computer forensics labs at the local level. It will also examine some of the technology, training and equipment available for use and their cost.

The local law enforcement agency has a duty and obligation to provide the highest level of service possible to their respective communities in meeting the demands of the 21st century. The establishment of computer forensics labs will enable local law enforcement agencies to meet the criminal and investigative challenges created by the Internet and to succeed in their responsibilities to their

communities. Administrators can use the capabilities provided by computer forensics labs to better allocate and manage resources. That a department's internal capabilities will be enhanced is without question; however, the external requirements of educating the community cannot be ignored. The community will benefit from this improved technology and education knowing that their local law enforcement agency is utilizing the most advanced technology to protect their families and assets.

REVIEW OF LITERATURE

One of the most important issues facing the law enforcement community today is the ability to detect, prevent, and prosecute criminal activities conducted via the Internet. According to Carter and Katz (1996), law enforcement has fallen behind in the computer age and regrettably fails to comprehend computer crime and the local impact that it has on communities. Computer networks have become a daily part of our lives, providing convenience in areas such as automatic teller machines, telephone calls and credit card purchases. Computer networks have become a haven for criminal activity in areas such as child pornography, solicitation of minor children, stalking, theft, and espionage. The law enforcement community needs to be educated that computers and their networks can contain evidence of violent crimes; including homicide, rape, arson, and abductions to name a few. An example is the following 1996 state of Maryland case study:

> October 1996 a Maryland woman, Sharon Lopatka told her husband that she was leaving home to visit friends in Georgia. Her husband became concerned when she did not return

> home within a few days, which caused him to contact the local police to make a missing person report. During the police department's investigation, it was discovered through examination of Sharon Lopatka's e-mail, there were 100's of e-mails between her and a Robert Glass. Examination of the e-mails between Sharon Lopatka and Robert Glass revealed that the two shared their fantasies about death and sexual acts of torture. Investigators located Robert Glass living in a trailer in North Carolina; he was located by his e-mail account. Sharon Lopatka's body was discovered in a shallow grave next to Robert Glass' trailer. She had been strangled to death and her hands and feet were tied. Robert Glass pled guilty at his trial and stated that Sharon Lopatka's death was an accident during sex (Casey, 2000, p. 1).

Computer forensics is the science of extracting data from computer systems and using the data to aid law enforcement in criminal investigations (Casey, 2000). This data extraction procedure is very complex and requires specialized computer hardware and software, magnetic storage capability and specialized training for personnel, all of which represents a substantial monetary expenditure (Phelan, 1995). Due to the required monetary expenditures for equipment and personnel, most local agencies have not created a computer forensics lab. Currently and for approximately the past ten to fifteen years, the majority of computer forensics labs are located at the federal agency level. The labs are not just located with the Federal Bureau of Investigations (FBI), they are located within other federal agencies such as the Drug Enforcement Agency (DEA), and even the Environmental Protection Agency (EPA), (EPA Programs, 2004; DEA Programs, 2004). The federal government has established the National Regional Computer Forensics Labs (RCFL) program (a FBI affiliated program), at different locations through out the country (Garrison, 2003). These RCFL locations focus entirely on the examination of digital evidence. The FBI affiliated RCFL locations currently are established in Dallas, Texas; San Diego and San Francisco, California; Kansas City, Missouri; Chicago, Illinois. According

to FBI Director Robert S. Mueller III, five additional RCFL's will be opened in 2004 at these locations; Houston, Texas; Buffalo, New York; Newark, New Jersey; Portland, Oregon; and Salt Lake City, Utah (Garrison, 2003). Part of the mission of each RCFL is the training of surrounding law enforcement agency personnel and to provide free advice such as how an officer should proceed to properly bag and tag digital equipment. All of the RCFL analysts are FBI certified and the labs will be seeking accreditation from the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (Garrison, 2003). Garrison (2003) further reports that the RCFL's not only provide analysis of computers, they also examine any type of digital medium where data may be stored such as; personal digital assistants (PDA); cell phones; laptop computers; and digital cameras. According to Kansas City RCFL Director Thomas J. Maiorana, "Almost every thing today is stored on a computer or some other digital medium and if it has been stored, we can generally retrieve it" (Garrison, 2003, p. 11).

The solicitation and stalking of children via the Internet is not just a local problem, it crosses state lines and even sources outside the United States. Due to the complexity of this growing problem, the FBI has had agents posing as children on Internet chat rooms, in the anticipation of apprehending child solicitors and pedophiles. According to Larrabee (1998), in 1998 the FBI hired 60 employees with expertise in computers and spent $10 million to combat computer sex crimes. Ly (2003) reports the FBI in 1995 launched Operation Innocent Images, in its efforts to combat the peddling of child pornography or other sexually explicit material depicting children, via the Internet. During this

operation, the FBI recruited the help of 3 teenage girls (one was an agent's daughter), to teach agents how to communicate as teenage girls on the Internet, in their efforts to catch child predators. The agents estimate that at any given time, 20,000 pedophiles are online worldwide, attempting to make contact with potential victims (Ly, 2003). The program has resulted in 2,200 convictions nationwide for arranging to meet minors for sex or swapping child pornography (Ly, 2003). Larrabee (1998) reports that on July 12,1998 in Holden, Mass., a convicted sex offender from Michigan was arrested. According to police, he drove there to meet a 16-year-old girl that he had communicated with on an Internet chat room. Police stopped the girl as she ran towards the suspect's truck with a suitcase in-hand (Larrabee, 1998). In another incident, according to investigative reporter McCoy (2000), between October 1999 and June 2000, Pastor William Cabell of State College, Pennsylvania, consistently logged into an Internet chat room and exchanged e-mails with an "Addam 1984" who was supposed to be a 14 year old boy from New Jersey. During these e-mails in the chat room, the issue of sex was brought up and William Cabell had already identified himself as a 46-year-old man. William Cabell agreed to meet "Addam 1984" on June 28, 2000 at a fast food restaurant in Piscataway, N.J., however he was met by an undercover FBI agent and placed under arrest for crossing state lines to have sex with a minor (McCoy, 2000). The aforementioned incidents should serve as a chilling reminder of the potential dangers that await our children and other loved ones.

Another area that is increasingly becoming a financial burden to our

citizens and the business community, are the area of identity theft and personal account thefts. The Federal Trade Commission (FTC) received 161,819 complaints of identity theft in 2002 (Lynch & Husted, 2003). The FTC ranked the states by the amount of theft victims to populations of 100,000. The FTC ranked the top 5 states with their respective top city as: District of Columbia, 123.1 ratio, with 704 victims; California, 90.7 ratio with 30,738 victims state wide, with the top city of Los Angeles reporting 2,609 victims; Arizona, 88.0 ratio with 4,517 victims state wide, with the top city of Phoenix reporting 1,268 victims; Nevada, 85.3 ratio with 1,705 victims state wide, with the top city of Las Vegas reporting 1,165 victims, and Texas, 68.9 ratio with 14,357 victims state wide, with the top city of Houston reporting 2,654 victims (Lynch & Husted, 2003). Lee (2003) reports that approximately 3.3 million American consumers discovered that their personal information had been used to open fraudulent utility, credit card, or bank accounts, or the information was used to commit other crimes. According to a Federal Trade Commission report the fraudulent use of this information cost consumers $3.8 billion and collectively cost businesses $32.9 billion (Lee, 2003). Further, Lee (2003) reported that fraudulent new accounts caused losses to businesses and financial institutions an average of $10,200 a case and the average cost to the consumer was $1,180 and approximately 60 hours to repair their credit history.

According to Lee (2003), 6.6 million people fell victim to theft in 2002, through their existing accounts due to the theft of their financial records, stolen credit cards and A.T.M. cards. These account thefts caused $1.1 billion in losses

to consumers with 80 percent of the cases involving credit card fraud, which in turn caused $14 billion in business losses (Lee, 2003). The established account thefts, on average cost the consumer $160 and an average of 15 hours spent on repairing their accounts in contrast to the average of $2,100 a case in business losses (Lee, 2003).

Of the victims, half of them knew what method the thieves used to obtain their personal information. In a quarter of all cases, the victims report that the information was stolen either through the loss of a wallet or the mail. Some 13 percent of the victims said the information had been stolen in the course of another transaction or a purchase (Lee, 2003). According to Lowry (1998), “skimming” has become the fastest area of credit card fraud and is being utilized by organized crime, waiters and sales clerks. The “skimmer”, which is usually a waiter or sales clerk, swipes the victims’ credit card through a magnetic card reader, which the “skimmer” usually hides on their belt (Lowry, 1998). The magnetic card readers can be as small as a pager making it concealable and can be purchased over the Internet for as little as $100 (Lowry, 1998). Lowry (1998) cited one example at a Coco Pazzo Café, where a former waiter and two others were charged with $250,000 in credit card fraud. In some instances, thieves and organized crime groups pay waiters and clerks to steal credit card information, which is sometimes e-mailed to foreign countries such as Japan, which has lax credit card fraud laws (Lowry, 1998).

The ability to recognize digital evidence depends on the investigator’s knowledge of the type of crime committed and their understanding of where

potential evidence in computer systems may be found (Casey, 2000). The severity of the crime is a determining factor in whether the entire system or just the hard drive should be seized. When collecting evidence, one area that has come up for debate is whether the computer system should be turned off. Law enforcement generally is trained to unplug all power source cables rather than use the systems power switch, in the event it is connected to an explosive boobytrap or cause the internal destruction of the computer (Casey, 2000). Some of the advantages of digital evidence are: evidence can be duplicated exactly and a copy can be examined to avoid damaging the original, utilizing the proper tools it is readily detectable if the digital evidence has been tampered with or modified, it is difficult to destroy even if the files have been “deleted”, and when criminals attempt to destroy digital evidence, copies can remain in areas of the computer that the criminals are not aware of (Casey, 2000).

The use of digital cameras and crime scene diagramming software can present evidence as never before experienced (Mayo, 2003). Mayo (2003) reports the local law enforcement agency is constantly dealing with budget constraints and the newest available technology will always present the question, “Will we be able to afford it?” The initial expense of digital photography may be significant; however, this expense will be off set over time due to the amount of money saved (Mayo, 2003). According to Mayo (2003), 35mm film has been the choice of law enforcement for decades to document crime scenes, bookings, and accidents. Despite the long tenure of 35mm film within law enforcement, the cost of film adds up and can become a burden on the crime scene section as they

may become too consumed with cost factors and not take as many photos at a crime scene as may be required (Mayo, 2003). Another area that becomes a financial burden is the cost of processing the film. The cost is not only monetary; it also costs in resources such as time and manpower (Mayo, 2003). When film is processed at commercial sites, an officer will usually be required to be present to observe the processing to maintain the chain of evidence (Mayo, 2003). Some agencies send their film to county or state labs for processing, which may result in longer processing time and may present potential chain of custody problems (Mayo, 2003). The use of 35mm film does not allow for immediate feedback to the officer processing a crime scene, as the officer is not able to see what has been captured on the film (Mayo, 2003). Since the 35mm film must be processed, the crime scene officer may not be able to return to the crime scene at a later date if it was discovered that important areas were missed (Mayo, 2003). The use of digital photography allows for the immediate feedback to the officer as they can look at the LCD screen to see what type of image(s) they have captured and whether or not more photos should be taken before leaving the crime scene (Mayo, 2003). The use of 35mm film also requires that the photographs and negatives must be filed. The filing of the photographs will add another loss of resources, as personnel will be required to file and retrieve these items, when their time and skills could be better utilized (Mayo, 2003). Mayo (2003) further reports the use of digital photography in law enforcement is presently in use by the Lowndes County Sheriffs Office in Valdosta, Georgia, Grand Chute, Wisconsin Police Department, and the West Windsor, New Jersey Police

Department.

Galvin (2003) reports the crime scene diagramming software available today has the capability of measurements of 1/1000th of an inch. The programs today offer compatibility, whereas the officer can download data points taken with a Nikon Total Station into The Crime Zone, which is a program designed specifically for crime and crash scenes, according to Daniel Holstein, a senior crime scene analyst with the Las Vegas Metropolitan Police Department (Galvin, 2003). The Crime Zone software also offers standardized diagram symbols such as guns, bloodstains, or a body, which provides a jury with a better understanding of a crime scene. These types of diagrams are usually copied onto an 8.5 x 11-inch crime report and make useful references for other investigators, jurors, attorneys, and judges (Galvin, 2003). These types of diagrams can be significantly enlarged by using a large-format plotter, which can provide for an impressive courtroom presentation (Galvin, 2003). The use of these digital diagram programs can ensure that details of evidence at a crime scene are preserved, even though the case may not go to trial for years. This is extremely important since the crime scene can be completely destroyed (razing a building) or physically altered due to renovations. These programs are also used to help accident reconstructionists when investigating fatalities or incidents where a criminal act is involved. The use of these programs for complex crime scenes has proven to be more clear and accurate than hand drawn diagrams (Galvin, 2003). Detective Doug Jordan, supervisor of the Eugene, Oregon Police Department's Major Collision Team, recalled an incident where officers were in a

high-speed vehicle chase and a shooting (Galvin, 2003). This incident involved an armed robbery-kidnapping suspect, when during the police pursuit the suspect hit a police unit head on and then fled on foot. The fleeing suspect then turned towards an officer, at which time the suspect was shot by the officer and after being shot, the suspect continued to flee on foot. The suspect was later apprehended. According to Detective Jordan, “this was a huge crime scene with a lot of tire marks and vehicles to measure. Measuring this by hand would have been difficult, if not totally impossible” (Galvin, 2003, p.15). When processing this crime scene, Detective Jordan used the Total Station program to map the area’s approximately 500 data points (Galvin, 2003). These data points were then downloaded into the The Crash Zone program which enabled Detective Jordan to produce a detailed and scaled diagram of the scene that day, which normally would have taken days to complete by hand (Galvin, 2003). Some of the mapping software programs are capable of showing the scene as a three-dimensional image (3D imaging), which provides the opportunity to view the scene at different vantagepoints (Galvin, 2003). Detective Jordan feels that 3D imaging is indispensable when processing shooting scenes. According to Detective Jordan, during one shooting investigation involving the SWAT team, numerous rounds were fired. During this investigation it was necessary to show the trajectory of each round, as several rounds had hit area residences (Galvin, 2003). Detective Jordan stated, “I could show the path that each round traveled from the muzzle to the bullet hole. This really helped the shooting board understand what had occurred that night” (Galvin, 2003, p. 32).

It is important to address the growing problem of collecting and marking digital evidence. In this context it is imperative that prosecuting attorneys learn how to defend the use of digital evidence and to determine if the evidence is admissible in a court of law (Digital Evidence, Inc., 2004). The challenge to the admissibility of evidence retrieved from a computer system chat room and e-mail record, was determined in the United States vs. Tank and the state of Washington vs. Townsend (Digital Evidence, Inc., 2004). The law enforcement community must learn how to develop and process admissible digital evidence, as this could be critical in trials involving pedophiles, abductions, and homicides. According to Sassinsky (2003), the law enforcement community can better prepare itself by reviewing case law and numerous suggestions contained in a published government document called "U. S. Department of Justice Search and Seizure Guidelines, Computer Crime and Intellectual Property Section, Criminal Division" at www.usdoj.gov/criminal/cybercrime/searchiflg.html. Another legal aspect of great importance to law enforcement agencies in the state of Texas is the enactment of Texas House Bill 2703 (State of Texas House Bill 2703). Texas House Bill 2703 was passed by the Texas legislature in May 2003 and relates to "the testing of physical evidence, crime laboratory accreditation, and the admissibility of evidence examined or tested by a crime laboratory" (Barbara, 2004, p. 10). The enactment of House Bill 2703 required the amending of the state's Code of Criminal Procedure, Article 38.85, subsections (d) and (e) (Barbara 2004). The amended language to the Texas Code of Criminal Procedure 38.85 (CCP 38.85) subsection (d) essentially requires that in order for

the forensic evidence to be admissible, the Texas Department of Public Safety must certify the crime laboratory submitting the forensic evidence (Barbara 2004). The amended requirements to the CCP 38.85 subsection (e) basically require that the submitting agency preserves one or more separate samples for use by the defense attorney or under order of the convicting court and further that the agency will preserve all samples until all appeals in the case are final; however, this subsection expires September 1, 2005 (State of Texas House Bill 2703). Another area that was affected by House Bill 2703 is, Subchapter A, Chapter 411 of the Government Code requiring that; "the director (Department of Public Safety) by rule shall establish an accreditation process for crime laboratories, including DNA laboratories, and other entities conducting forensic analysis of physical evidence for use in criminal proceedings" (Barbara, 2004, p. 10). An item of specific interest is, the Texas Department of Public Safety's crime laboratories are and have been certified for a number of years by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) (Barbara, 2004). The ASCLD/LAB will consider a stand-alone section or unit for certification that is performing analysis in computer forensics, audio analysis, video analysis, and or imaging analysis (Barbara, 2004). Prior to submitting an application for ASCLD/LAB certification, the lab director must ensure that his/her laboratory can pass the essential criteria as outlined in the "2003 ASCLD/LAB Manual" (Barbara, 2004). The ASCLD/LAB manual describes the digital evidence section as having four sub-disciplines: computer forensics, imaging analysis, audio analysis, and video analysis (Barbara, 2004). For a stand-alone digital

evidence unit, this will entail documenting compliance with 102 criteria elements of the “2003 ASCLD/LAB Manual” (Barbara, 2004).

It is abundantly clear; law enforcement agencies across the entire spectrum must train their personnel in the area of computer forensics. Numerous companies/organizations have come into existence to serve the needs of the law enforcement community and private industry (IACIS, 2004). One such organization is the International Association of Computer Investigative Specialists (IACIS). The IACIS is an international volunteer non-profit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science. Law enforcement professionals ranging from local to international agencies represent the membership of IACIS (IACIS, 2004). The training offered by IACIS is in the areas of seizure and processing computer systems. The training further introduces forensic methods in searching computer systems, ensuring that the rules of evidence and the laws of search and seizure are learned. The IACIS program also provides for learning methods of detecting evidence that has been hidden, encrypted, protected with passwords or destruction devices that could destroy the evidence or the physical computer (IACIS, 2004). The IACIS offers two certifications, Certified Electronic Evidence Collection Specialist and Certified Forensic Computer Examiner, with recertification required every three years. The training is offered at different locations throughout the year and the cost is $1395.00, which does not include travel expenses (IACIS, 2004). The staff of the IACIS may not receive any outside compensation or gratuity due to the non-profit status, and all staff

members, board members and instructors have all their expenses paid for by the IACIS (IACIS, 2004).

An informal survey of 7 municipal agencies within the Dallas/Fort Worth Metroplex area was conducted, which are used in research as a “measuring device” of similar sized cities, by the Mesquite Police Department. The survey asked respondents if their agency: had a forensics lab, if their agency provided an officer(s) to the FBI Dallas Regional Computer Forensics Lab (RCFL), did their department participate in the 3 year intern program with the Dallas RCFL, and did their department use the Dallas RCFL for processing. The survey provided the following information: 5 departments either had their own forensics lab or were in the process of establishing one, 3 departments had officers assigned to the Dallas RCFL, 2 departments had officers to complete the 3 year intern program with the Dallas RCFL, and all agencies use the Dallas RCFL for the more complicated cases. An informal survey within a Module I of the Law Enforcement Management Institute of Texas (LEMIT) was conducted of 20 different agency attendees. The survey asked respondents to provide the following information: number of sworn officers, population of jurisdiction, does the agency have a forensics lab, how many sworn officers are assigned to the lab, does your agency now or in the past assign officers to the local area RCFL, what agency provides computer forensics lab support to your department, and which of these crimes does your agency use computer forensics labs for an investigative tool, narcotics, missing persons, pedophiles, identity theft through the Internet, homicides, child pornography, theft through the Internet, and crime scene processing. The survey

provided the following information: number of sworn officers ranged from 12 to 1250, population ranged from 1,000 to 750,000, 4 agencies had their own computer forensics lab, whereas 16 agencies did not, 1 agency had 8 sworn officers assigned to a lab, 1 agency had 3 sworn officers assigned to a lab, and 2 agencies had 1 officer assigned to a lab, 18 agencies do not currently or have in the past assigned an officer to the local area RCFL whereas 2 agencies have made such assignments. The FBI or the Texas Department of Public Safety generally has provided support for those agencies without labs. The crime areas the agencies used computer forensics labs were: 14 agencies utilized the service for child pornography, 13 agencies for investigating pedophiles, 10 agencies for investigating identity theft through the Internet, 9 agencies for investigating theft through the Internet, 7 agencies for investigating narcotics, 5 agencies for crime scene processing, 4 agencies for investigating homicides, and 3 agencies for missing persons cases.

An informal interview was conducted with Z. LaJoie, the City of Mesquite Information Systems manager, in which he was asked to review the Mesquite Police Department's current computer systems capabilities, to make a recommendation for required upgrades, potential equipment vendors, and estimated expenses to establish a computer forensics lab. Accordingly, Z. LaJoie (personal communication, August 19, 2003) provided 3 estimates from multiple vendors to build the system for a short term solution (1-2 years): Commercial RAID Box with 3.75 trillion bytes of storage capacity for $7,041.22, SCSI system with 720 giga bytes of storage capacity for $2,523.00, and IDE system with 960

giga bytes of storage capacity for $1012.00. Z. LaJoie (personal communication, August 19, 2003) recommended the purchase of the IDE system due to price and performance.

METHODOLOGY

The purpose of this project is to explore if computer forensics labs should be established at the local law enforcement level to enhance their investigative capabilities in providing service to their communities. It is hypothesized that a computer forensics lab will greatly enhance local law enforcement agency's capabilities to investigate crimes. These enhanced investigative capabilities include white-collar crimes, abductions, homicides, crimes committed against children and this is not an all-inclusive list. Furthermore, the aspects of crime scene processing will be dramatically changed in procedures and processes. It is also hypothesized that a need exists to educate the community of their vulnerability on the Internet and actions that Internet users can initiate to protect their children and their assets.

This project utilizes Internet search, magazines, and police periodicals to conduct a review of literature on information concerning computer forensics labs. An informal survey was conducted of twenty-law enforcement agencies (outside of the Dallas/Fort Worth Metroplex area), which ranged in populations of 1,000 to 750,000 and the agencies consisted of municipal, county sheriff's departments and departments of public safety for a large hospital and university. The informal survey was also conducted with 7 cities within the Dallas/Fort Worth Metroplex area, which are used in research as a "measuring device" of similar sized cities

by the Mesquite Police Department. An informal interview was also conducted with the City of Mesquite Information Systems manager.

In the informal survey of the twenty-seven departments, information was requested if the respective department had a computer forensics lab, if not, who provided the service for them (if any), and the basic types of investigations for which the lab was used.

In the informal interview conducted with the City of Mesquite, the Information Systems manager was asked to review the police department's current computer systems capabilities, to make a recommendation for required upgrades, potential equipment vendors and estimated expenses to establish a computer forensics lab within the Mesquite Police Department.

FINDINGS

It is readily apparent with the introduction of computers into our society, they have become a part of our every day lives, being utilized for legal and illegal activities. The Internet (Cyberspace) has created a dependence on information technology and information infrastructure, which has evolved into a threat to our national security and economy (The National Strategy to Secure Cyberspace, 2003). According to the National Strategy to Secure Cyberspace (2003), the critical components of the nation's infrastructure are; banking and finance, postal and shipping, agriculture, food, water, government, chemicals and hazardous materials, public health, emergency services, and the defense industrial base. Accordingly, local law enforcement has become a critical element in the national security (The National Strategy to Secure Cyberspace, 2003). The National

Strategy to Secure Cyberspace (2003) further stressed that local law enforcement agencies must attempt to control the criminal element through prosecution, to aid in protection of the nation's infrastructure.

Due to the vast increase in computer technology, potential threats to national security, and the illegal activities conducted on the Internet, the establishment of computer forensics labs has evolved. Computer forensics is the science of extracting data from computer systems and using the data to aid law enforcement in criminal investigations (Casey, 2000). These types of labs will provide investigative information that was not previously available, better management of resources and quality service to the community. Computer forensics labs provide advance technology for crime scene processing, through the use of digital photography, digital crime scene diagramming, and the ability to analyze computer data in cases that involve pedophiles, homicides, financial crimes, theft, forgeries, and identity theft on the Internet (Casey, 2000). The solicitation and stalking of children on the Internet is not just a local problem, it crosses state lines and even sources outside the United States (McCoy, 2000). An area that is increasingly becoming a financial burden to our citizens and the business community are the areas of identity theft and personal account thefts. Lee (2003) reported that American consumers discovered that their personal information had been used to open fraudulent utility accounts, credit card accounts, or the information was used to commit other crimes.

In reviewing information from Internet search, books dedicated to computer forensics labs, periodicals and informal surveys of selected law

enforcement agencies, local law enforcement agencies have been extremely slow in establishing these types of labs. According to Carter and Katz (1996) law enforcement has fallen behind in the computer age and regrettably fails to comprehend computer crime and the local impact that it has on communities. While these types of labs have been in existence for over 10-years at the federal government level, local law enforcement agencies as a whole have been reluctant to establish their own labs primarily due to costs (Phelan, 1995). The federal government has established the National Regional Computer Forensics Lab (RCFL) program (an FBI affiliated program), at different locations throughout the country (Garrison, 2003). These RCFL locations focus entirely on the examination of digital evidence.

The law enforcement community must learn how to develop and process admissible digital evidence, as this could be critical in trials involving pedophiles, abductions, and homicides according to Sassinsky (2003). Prosecuting attorneys must learn how to defend the use of digital evidence and to determine if the evidence is admissible in a court of law (Digital Evidence, Inc., 2004). The ability to recognize digital evidence depends on the investigator's knowledge of the type of crime committed and their understanding of where potential evidence in computer systems may be found (Casey, 2000). According to Casey (2000), some of the advantages of digital evidence are: when criminals attempt to destroy digital evidence copies can remain in areas of the computer that the criminals are not aware of, digital evidence is difficult to destroy even if the files have been "deleted", evidence can be duplicated exactly and a copy can be

examined to avoid damaging the original, and utilizing the proper tools it is readily detectable if the digital evidence has been tampered with or modified. The use of digital cameras and crime scene diagramming software can present evidence as never before experienced (Mayo, 2003). The initial expense of digital photography may be significant; however, this expense will be off set over time due to the amount of money saved (Mayo, 2003). The use of digital photography allows for the immediate feedback to the officer as they can look at the LCD screen to see what type of image(s) they have captured and whether or not more photos should be taken before leaving the crime scene (Mayo, 2003).

Galvin (2003) reports the crime scene diagramming software available today has the capability of measurements of 1/1000th of an inch. The programs today offer compatibility, whereas the officer can download data points taken with a Nikon Total Station into The Crime Zone, which is a program designed specifically for crime and crash scenes (Galvin, 2003). The Crime Zone software also offers standardized diagram symbols such as guns, bloodstains, or a body, which provides a jury with a better understanding of a crime scene (Galvin, 2003). The use of these programs for complex crime scenes has proven to be more clear and accurate than hand drawn diagrams (Galvin, 2003).

Numerous companies/organizations have come into existence to serve the needs of the law enforcement community and private industry in the area of Cyberspace illegal activities and security breaches (IACIS, 2004). One such organization is the International Association of Computer Investigative Specialists (IACIS). The IACIS program provides for learning methods of detecting evidence

that has been hidden, encrypted, protected with passwords or destruction devices that could destroy the evidence or the physical computer (IACIS, 2004). The IACIS offers two certifications, Certified Electronic Evidence Collection Specialist and Certified Forensic Computer Examiner, with recertification required every three years. The training is offered at different locations throughout the year and the cost is $1395.00, which does not include travel expenses (IACIS, 2004).

The informal survey of 7 municipal agencies within the Dallas/Fort Worth Metroplex area showed that of agencies comparative in size to the Mesquite Police Department, 5 departments have or are in the process of establishing these labs. Furthermore, of these 5 agencies, all have had or currently have an officer assigned to the Dallas-RCFL 3-year internship program. The informal survey of 20 different agencies, which varied from municipal, county sheriffs departments and university departments of public safety, reflected that 16 agencies do not have a lab established or plans to institute one. The survey further indicated that of the 4 agencies that have established labs, only 2 departments participated in their areas RCFL internship program. The informal interview conducted with the City of Mesquite Information Systems manager (personal communication, August 19, 2003), indicates that the equipment costs for systems upgrades of the department's current computer systems would be $1012.00, should the department accept the recommendation to purchase the IDE system. The recommended upgrades (if implemented) would meet the requirements of the Mesquite Police Department for the next 2 years, as far as

technology is concerned.

DISCUSSION/CONCLUSIONS

The purpose of this project is to explore if computer forensics labs should be established at the local law enforcement level to enhance investigative capabilities in providing service to their communities. It is hypothesized that a computer forensics lab will greatly enhance local law enforcement agencies' capabilities to investigate crimes. These enhanced investigative capabilities include white-collar crimes, abductions, homicides, crimes committed against children and this is not an all-inclusive list. Furthermore, the aspects of crime scene processing will be dramatically changed in procedures and processes. It is also hypothesized that a need exists to educate the community of its vulnerability on the Internet and actions that Internet users can initiate to protect their children and their assets.

When reviewing the different literature, the importance of local law enforcement's involvement in prosecuting crimes committed via the Internet (Cyberspace), in the area of national security had not been considered. According to the National Strategy to Control Cyberspace (2003), the introduction of computers into our society, our dependence upon the information technology and the information infrastructure of the Internet (Cyberspace), have become a threat to our national security. This threat is to the nervous system of the nation's critical infrastructures and the control system of our country, which is Cyberspace (The National Strategy to Control Cyberspace, 2003).

The existence of computer forensics labs for over 10-years at the federal

government level and local law enforcement's reluctance to establish these types of labs (Phelan, 1995) was an unexpected development. Furthermore, local law enforcement's failure to comprehend computer crime and the local impact that it has on communities (Carter & Katz, 1996) was another unexpected finding.

The use of digital photography and digital crime scene processing software can present evidence as never before experienced, such as 3-dimensional diagramming and photography (Mayo, 2003). The use of these programs can produce quality diagramming that has proven to be more accurate than hand drawn diagramming, even to 1/1000th of an inch (Galvin, 2003). The use of crime scene programs such as Crime Zone and the Nikon Total Station, provides the capability of using standardized reference symbols such as bloodstains, a body or a weapon which provides jurist with a better understanding of the crime scene (Galvin, 2003). The use of these digital programs will provide immediate feedback, so officers at a scene can see if they have captured the required images and measurements. The digital programs allow for better storage and capture the images (photography) as they were at the time of the offense, which can be of real importance should the scene be altered later, such as the razing of a building. The initial cost of digital photography may be significant, however the cost will be off set in time due to the savings in man-hours, storage costs and processing fees (Mayo, 2003).

It is readily apparent that computer forensics labs should be established at the local level or the services that these labs provide are received from an outside source. The local governmental bodies and the top law enforcement

administrators must address whether to establish computer forensics labs within their agencies or find a viable external support system to provide this service such as the Regional Computer Forensics Labs (RCFL) which are provided by the federal government. Police administrators must train their personnel to understand how computers and related systems can be used in criminal activities; then the agency is properly trained and has the proper mental attitude to meet the demands of the 21st century. These types of labs provide investigative capabilities and information that has not been previously available. The vulnerability of communities, individuals and especially children due to illegal activities conducted via the Internet has brought a new dimension of responsibility to the local law enforcement agency. This responsibility is not just to the communities they serve, but the national security as well. Police administrators must become familiar with and fully grasp the concept(s) of how crime can be committed against their communities via the Internet, even though the suspects are not located in the local area. The police administrator must ensure that local government officials fully understand the importance of investigating and prosecuting crimes committed via the Internet, with the expectation(s) to receive favorable action during the budget process. Perhaps the computer forensics lab discussion will provide local government officials and police administrators the realization of the benefits of the 21st century and it's pitfalls, and how their responsibility to their communities must include educating the community on how to protect their families and assets.

REFERENCES

Barbara, J. (2004). Digital evidence accreditation. *Law Enforcement Technology, February 2004*, 8-15.

Casey, E. (2000). *Digital evidence & computer crime.* California: Academic Press, 1,4-5,12,48.

Digital Evidence Incorporated. (2004). Authenticating evidence of Internet chat room logs recovered from a hard drive. Retrieved January 21, 2004, http://www.digital-evidence.com/news/recent_cases.asp

Donofrio, A. (2002). Computer forensics & analogies. *Law Enforcement Technology, 29-*(1), 64-69.

Galvin, B. (2003). Drawing conclusions. *Evidence Technology Magazine, 1-(*4) 14-15, 32.

Garrison, D. (2003). Regional computer forensics laboratories. *Evidence Technology Magazine, 1-*(4), 10-13.

International Association of Computer Investigative Specialists. (2004). *About IACIS.* Retrieved January 21, 2004, http://www.cops.org/

Larrabee, J. (1998, August). New beat for local police: The Internet. *USA Today*, 8.

Lee, J. (2003, September). Identity theft victimizes millions, costs millions [Electronic Version]. *The New York Times,* retrieved September 4, 2003.

Lowry, T. (1999, June). Thieves swipe credit with card readers. *USA Today*, 1B.

LY, P. (2003, June). Maryland teens help FBI catch pedophiles on the Internet. *The Washington Post*, A7.

Lynch, C., & Husted, B. (2003, March). ID thieves turn sights toward businesses. *Atlanta Journal Constitution*, G1, G7.

Mayo, K. (2003). From film to digital. *Evidence Technology Magazine, 1-*(4) 29-30.

McCoy, F. (2000, August). The web's dark side: Child solicitation. U*.S. News & World Report*, 42-43.

Mendell, R. L. (1998). *Investigating computer crime: A primer for security managers.* Springfield, Illinois: Thomas, Charles C., Publisher Ltd.

Phelan, M. J. (1995). Computer forensics and expert system technology. *Counter Drug Law Enforcement: Applied Technology for Improved Operational Effectiveness International Symposium, (1)*-4-44. Abstract retrieved September 18, 2003, from (NCJ Publication No. 162647) Washington DC: U.S. Government Printing Office.

Sassinsky, J. (2003, March). How law enforcement uses computer forensics in modern investigations [Electronic Version]. The *New York Law Journal-Techtrends.* Retrieved January 22, 2004 from http://www.sassinsky.com/caught.html

State of Texas House Bill 2703: *Relating to the testing of certain physical evidence, crime laboratory accreditation and the admissibility of evidence examined or tested by a crime laboratory*. Retrieved February 19, 2004, from http://www.capitol.state.tx.us/cgi-bin/tlo/viewtext.cmd

Stephenson, P. (1999). *Investigating computer-related crime.* Boca Raton, Florida: CRC Press.

The White House. (2004). *The national strategy to secure cyberspace.* [Electronic Version]. Retrieved April 11, 2004, http://www.whitehouse.gov/pcipb

U. S. Drug Enforcement Administration. (2004). *Computer forensics program.* Retrieved January 21, 2004, http://www.usdoj.gov/dea/programs/cfp.htm

U. S. Environmental Protection Agency. (2004). *Computer forensics.* Retrieved January 21, 2004, http://www.epa.gov/compliance/criminal/forensics/computer